НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210219.3 | 19 февраля 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольных команд в VMware vSphere Replication

Идентификатор уязвимости	MITRE: CVE-2021-21976
Идентификатор программной ошибки	CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (Внедрение команд ОС)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольные команды в целевой системе посредством отправки специально сформированного вредоносного запроса со страницы "Startup Configuration". Уязвимость обусловлена некорректной обработкой входных данных.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	VMware vSphere Replication до v8.3.1.2, 8.2.1.1, 8.1.2.3, 6.5.1.5
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	11 февраля 2021 г.
Дата обновления	11 февраля 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	7.2 AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Высокий (H)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
Масштаб последствий эксплуатации уязвимости (S)	Не изменяется (U)
Влияние на конфиденциальность (C)	Высокое (H)

Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.vmware.com/security/advisories/VMSA-2021-0001.html https://www.cybersecurity-help.cz/vdb/SB2021021201